KUTSESTANDARD

Infoturbespetsialist, tase 5

Kutsestandard on dokument, milles kirjeldatakse tööd ning töö edukaks tegemiseks vajalike oskuste, teadmiste ja hoiakute kogumit ehk kompetentsusnõudeid. Kutsestandardeid kasutatakse õppekavade koostamiseks ja kutse andmiseks.

Kutsenimetus	Eesti kvalifikatsiooniraamistiku (EKR) tase
Infoturbespetsialist, tase 5	5

A-osa
KUTSEKIRJELDUS

A.1 Töö kirjeldus

Infoturbespetsialist viib ellu organisatsiooni infoturvapoliitikat ning juhindub infoturbevaldkonna heast tavast. Ta pakub välja ja rakendab varadele vajalikud turvameetmed. Ta juhendab, toetab ja informeerib kaastöötajaid, et tagada infosüsteemide turvaline toimimine.

Tüüpiliselt töötab infoturbespetsialist organisatsioonis, kus infosüsteemid ja IT-lahendused moodustavad olulise osa asutuse varadest ning kus äriprotsessid on olulises sõltuvuses infosüsteemidest ja rakendustest, kus äriandmeid kogutakse ja hallatakse IT-süsteemide abil.

Infoturbespetsialisti kutse kirjeldamise aluseks on Euroopa IKT-kompetentside raamistik (e-CF).

5nda taseme infoturbespetsialist töötab mitmesuguste IT-süsteemide ja tööriistadega. Ta juhendab kaastöötajaid infoturbealaselt ning vajadusel juhib ka väikest meeskonda. Väikeettevõttes töötab infoturbespetsialist tavaliselt iseseisva infoturbespetsialistina. Suures ettevõttes töötab infoturbespetsialist kas infoturbe- või IT meeskonnas.

5nda taseme infoturbespetsialist töötab keskkonnas, kus tehnoloogiad muutuvad, täiustuvad ning vahetuvad väga kiiresti. Intsidentide või suurarenduste perioodidel on töö kiire ja pingeline, otsustusi tuleb teha piiratud info põhjal. Töö iseloom võib nõuda valveaega või erakorralist reageerimist tööaja väliselt.

5nda taseme infoturbespetsialistil on hea ülevaade operatsioonisüsteemidest, võrgust, turbe- ja standardtarkvarast. Ta oskab kasutada skriptimisvahendeid, protsesside kirjeldamise ja projekteerimise tööriistu ning versioonihalduse vahendeid. Ta on teadlik tunnustatud infoturberaamistikest ja standarditest (s.h. EITS ja ISO/IEC 27001) ning vajadusel suudab neid organisatsioonis rakendada. Ühtlasi on ta teadlik EL isikuandmete kaitse üldmääruse GDPR sätetest ning suudab edendada selle tuge seadmetes, infosüsteemides ja rakendustes (vt standard ISO 19944). Ta tunneb küberturvalisust puudutavaid seadusakte.

Infoturbespetsialisti töö eeldab loogilist mõtlemist, analüüsivõimet, algatusvõimet, suhtlusvõimet, kohusetunnet, seaduskuulekust, keskendumisvõimet, laia silmaringi, oskust töötada metoodiliselt ning olla orienteeritud detailidele. Vajalik on inglise keele oskus, kriitilise mõtlemise võime ning suutlikkus töötada meeskonnas ja vastuoluliste nõuete tingimustes. Infoturbespetsialist suudab vajaduse tekkides ning inglise keeles suhelda küberintsidenti puutuvate asutuste ja organisatsioonidega välisriikides, sh isikutega, kelle ametialane positsioon on oluliselt erinev.

Seoses juurdepääsuga kriitilistele süsteemidele ning konfidentsiaalsele teabele on eetikanõuded tavapärasest kõrgemad. Paljudel infoturbega seotud töökohtadel on püstitatud taustakontrolli või riigisaladuse juurdepääsuloa nõue.

Kutsestandardi erialaterminoloogia on viidud vastavusse erialasõnastikuga AKIT (akit.cyber.ee).

A.2 Tööosad
A.2.1. Sisendi andmine IKT rakenduse projekteerimisse/kavandamisse (e-CF kompetents A.6.) A.2.2. Tehnoloogia arengu jälgimine (e-CF kompetents A.7.) A.2.3. Komponentide integreerimine süsteemi (e-CF kompetents B.2.) A.2.4. Kliendile pakutava toote testimine (e-CF kompetents B.3.) A.2.5. Lahenduse paigaldamine (e-CF kompetents B.4.) A.2.6. Dokumentatsiooni koostamine (e-CF kompetents B.5.) A.2.7. Kasutajatugi (e-CF kompetents C.1.) A.2.8. Muudatuste tugi (e-CF kompetents C.2.) A.2.9. Teenuse andmine (e-CF kompetents C.3.) A.2.10. Intsidendi- ja probleemihaldus (e-CF kompetents C.4.) A.2.11. Infoturbestrateegia väljatöötamises osalemine (e-CF kompetents D.1.) A.2.12. Personaliarendus (e-CF kompetents D.9.) A.2.13. Riskihaldus (e-CF kompetents E.3.) A.2.14. Infoturbe haldamine (e-CF kompetents E.8.)
A.3 Kutsealane ettevalmistus
Infoturbespetsialistil on vähemalt keskharidus ning varasemalt (kutseõppe tasemeõppes, IKT-alasel täiendkoolitusel või töökohal) omandatud 4nda taseme IT-süsteemide spetsialisti kompetentsid.
A.4 Enamlevinud ametinimetused
Infoturbespetsialist, küberturbe spetsialist, infoturbeekspert, IT-turvaspetsialist, küberturvalisuse konsultant, turvalahenduste haldur (SIEM, tulemüür, IDS/IPS jm.), seirespetsialist.
A.6 Tulevikuoskused
Teave oskuste ja trendide kohta, mille tähtsus valdkonnas kasvab. Globaalsed väärtus- ja tarneahelad on pidevas muutumises. Igapäevaseks on muutumas IT-vahendite tarneahela ründed, tekkimas on uued ohuagendid („ründeriistad müügiks" tüüpi firmad) ning on vaja kasvatada jätkusuutlikkust (business continuity) ja kerksust (resilience). E-riigi elemendid (kesksed andmebaasid, e-valitsemine, elektrooniline isikutuvastus, e-pangandus, e-meditsiin ja e-kaubandus) on jõudmas üha enamatesse riikidesse (ka arengumaadesse), mistõttu vajadus usaldusväärse infoturbealase tööjõu järele tõuseb lähiaastatel jätkuvalt. Oluliselt tõuseb ka rakenduste ja lahenduste arv ning keerukus. Infoturbespetsialistil tuleb arvestada järgmiste tulevikusuundumustega ning end neis valdkondades täiustada ning töö kõrvalt pidevalt oskusi juurde õppida: 1. Serverite virtualiseerimine, klastrid, arvutikeskkonna loomine tarkvara abil (Kubernetes, Ansible). Praktikas on DevOps'i ja infoturbe roll sageli ühildatud (DevSecOps). 2. Pilvetehnoloogiad; pilvteenuste alane murrang Eestis toimus aastal 2022, üha rohkem organisatsioone püstitab rahalistel kaalutlustel oma IT-taristu pilve, mis aga eeldab vastavust turva- ja privaatsusnõuetele. 3. Ülemaailmsed identiteedihalduslahendused muutuvad üha olulisemaks, neid haldavatele firmadele rakendatakse piiranguid (Digital Markets Act, „gatekeeper"), digitaalset isikutuvastust (eIDAS 2, digikukkur) reguleeritakse üha täpsemini. 4. Seoses kvantarvutite arenguga on ette näha traditsiooniliste krüptograafiliste algoritmide murdumist ning vajadust nende asendamiseks postkvant-krüptograafiaga. Infoturbespetsialist peab mõistma krüptograafia olulist rolli tänases digimaailmas. 5. Suurandmed ja nende analüüs, neurovõrgud ja masinõppe algoritmid, tehisintellekti abiga genereeritav pilt ja heli (sh süvavõltsingud), mis muudavad võimatuks senituntud usaldusfaktoritele (sh biomeetria) tuginemise ning tingivad vajaduse täiendavate digitaalsete usaldusahelate sisseseadmiseks. 6. Tehisintellekti kasutamine oma töös, sh. IT lahenduste kaitseks. 7. Väga kiired arengud digitaalraha valdkonnas (sh EL). 8. Küberruum on muutunud rahvusvahelise vastasseisu tandriks, kus toimuvad küberründed ja tarneahelate ründed ning nn standardisõjad ja rakendatakse vastastikusi sanktsioone. 9. Üha rohkem on EL tehnoloogiaalaseid määrusi ja direktiive (GDPR, NIS 2, eIDAS 2, Digital Markets Act), mis mõjutavad IT süsteeme otseselt.

10. Insenerid/tehnikud ning juristid on infoturbes tegutsenud omal kitsal erialal, kuid on märke, et neil tuleb asuda koostööle, et tagada GDPR tugi ning tehnilistesse lahendustesse vaikimisi lõimitud andmekaitse. 11. Üha rohkem mõjutatakse inimeste käitumist psühholoogiliste võtetega, mille tagajärjel nad eiravad infoturvareegleid- suhtlusründeid oleks palju raskem läbi viia, kui kasutaja saab nende olemusest aru ja näeb ründe läbi. 12. IT'd kasutatakse üha enam elukeskkonna parendamisel (nutikad teed, esemevõrk, automatiseeritud tootmine, kaugtöö, ringmajandus), mis samuti vajab turvet.

B-osa
KOMPETENTSUSNÕUDED

B.1 Kutse struktuur
Infoturbespetsialisti kutse taotlemisel tuleb tõendada kõik kohustuslikud kompetentsid B.3.1.-B.3.14. ja üldoskused B.2.

B.2 Infoturbespetsialist, tase 5 üldoskused
Mõtlemisoskused 1. Kasutab mõtlemisel loogikat ja süsteemset arutlust, et näha nähtustevahelisi seoseid, teha järeldusi, tuvastada alternatiivsete lahenduste tugevad ja nõrgad küljed ning leida probleemide võimalikud lahendamise viisid. 2. Suudab hinnata teabe, argumentide jne kvaliteeti, töötleb ja mõistab faktide ja faktiseoste kõige olulisemaid aspekte. 3. Tuvastab ja sõnastab tekkida võivad ning juba tekkinud probleemid. Hindab lahenduse leidmise võimalusi ja strateegiaid. 4. Pakub uusi ja innovaatilisi mõtteid, märkab vajakajäämisi ning pakub nende lahendamiseks uusi viise ja võimalusi. 5.Omandab uusi teadmisi ja oskusi. Mõtestab ja väärtustab õpitu sisulist tähendust. 6. Jälgib valdkonnas toimuvaid muutusi ja suundumusi, et olla kursis tehnoloogia, meetodite jm uuendustega. Enesejuhtimisoskused 1. Järgib tööd tehes juhiseid, valdkondlikke nõudeid, eeskirju, õigusakte, standardeid, konventsioone jmt. 2. Järgib oma tegevuses nii isiklikke, ühiskondlikke kui ka organisatsiooni väärtusi ja põhimõtteid, kasutab organisatsiooni ressursse vastutustundlikult ja heaperemehelikult. 3. Kohaneb ootamatute olukordadega kiiresti ja paindlikult, leiab lahendusi ning säilitab adekvaatse tegutsemisvõime. 4. Määratleb oma koolitusvajaduse ja arendab end oma arengueesmärkide saavutamiseks (nt osaleb erialaüritustel, koolitustel, kutseühingute tegevuses, loeb erialakirjandust, tutvub uute seadmete ja programmidega). 5. Kasutab oma tegevuses enda ja teiste tervist säästvaid tööviise, isikukaitsevahendeid ning järgib ohutusnõudeid. Lävimisoskused 1. Tegutseb ühiste eesmärkide saavutamise nimel. 2. Oskab tagasisidet anda tasakaalukalt. Klientide ja kaastöötajatega suhtleb heast tavast lähtudes. 3. Väljendab end ka keerukates suhtlusolukordades viisakalt, arusaadavalt ja olukorrale vastavalt, mõistab teise mõtteid ja seisukohti. 4. Esitab asjakohast teavet selgelt ja arusaadavalt nii suuliselt, kirjalikult kui ka visuaalselt. 5. Kasutab suhtlemisel ja dokumentide koostamisel korrektset terminoloogiat. 6. Valdab eesti keelt tasemel B2, vene või inglise keelt tasemel B1 (vt Lisa 1 "Keelte oskustasemete kirjeldused"). 7. Kasutab arvutit tasemel "Vilunud kasutaja" (vt Lisa 2 „Digipädevuste enesehindamise skaala").

B.3 Kompetentsid	
B.3.1 Sisendi andmine IKT rakenduse projekteerimisse/kavandamisse (e-CF A6)	**EKR tase 5**
Tegevusnäitajad 1. Osaleb organisatsiooni äriprotsesside turvalisuse tagamises, sh uute rakenduste kavandamises ning olemasolevate uuendamises.	

2. Sõnastab kavandatava süsteemi turvanõuded ja turvatingimused, aitab koostada süsteemi mittefunktsionaalnõudeid (NFR). 3. Pärast süsteemi teostamist verifitseerib nõuete täidetuse (ülevaatuse ja testimise teel).	
B.3.2 Tehnoloogia arengu jälgimine (e-CF A7)	**EKR tase 5**
Tegevusnäitajad 1. Hoiab end kursis IT-alaste uudiste ja tehnoloogiliste uuendustega, samuti turvanõrkuste, andmelekete ning krüptograafia alaste uudistega, värskete turvaohtude ja kaitsemeetoditega; jälgib uudiskirju, ohukirjelduste vooge ning muid organisatsiooni infoturbe jaoks olulisi teabekanaleid. 2. Teavitab IT-meeskonda ja vajadusel juhtkonda talle teatavaks saanud ning äri mõjutada võivatest turvakeskkonna muutustest.	
B.3.3 Komponentide integreerimine süsteemi (e-CF B2)	**EKR tase 5**
Tegevusnäitajad 1. Paigaldab infoturvet tagavad või parendavad seadmed, tarkvara või alamsüsteemi komponendid käitatavasse või evitatavasse süsteemi, järgib seejuures infoturbe head tava ning muudatustehalduse protseduure. 2. Teeb süsteemist või selle osast varukoopiad, tagab süsteemi tervikluse integratsiooniprotsessis. 3. Testib evitatud süsteemiosa funktsionaalset toimimist ja jõudlust. 4. Koostöös IT meeskonnaga tagab paigaldatud süsteemi, riistvara, tarkvara või komponendi jätkuva turvalisuse (andmete konfidentsiaalsuse ja tervikluse ning süsteemi käideldavuse).	
B.3.4 Kliendile pakutava toote testimine (e-CF B3)	**EKR tase 5**
Tegevusnäitajad 1. Koostab ja hindab IKT süsteemide testimise protseduure (sh eelmisele versioonile naasmise protseduure) ning sooritab testimist nende protseduuride alusel, arvestades infoturvanõudeid, testimisprotsessi elutsüklit ning testimise liike. 2. Hindab infoturbe aspektist toote kasutatavust, jõudlust, töökindlust ja ühilduvuse aspekte ettevõttesiseste ja -väliste, riigisiseste ja rahvusvaheliste standardite valguses. 3. Koostab töödokumente ja -aruandeid, vajadusel tõendab infoturvameetmete ja IT-lahenduse vastavust infoturbealastele sertifitseerimisnõuetele. 4. Osaleb toote läbistustestimise korraldamisel turvalisuse parendamise eesmärgil.	
B.3.5 Lahenduse paigaldamine (e-CF B4)	**EKR tase 5**
Tegevusnäitajad 1. Plaanib ja organiseerib paigaldamise ja seadistamise, arvestades evituse ja olemasoleva arhitektuuri koosmõju. 2. Koostöös IT meeskonnaga, seadistab paigaldatud süsteemi (sh võrk, serverid, andmebaasid, veeb ja pilv) vastavalt turvanõuetele. 3. Kaasab täiendavaid erialaseid ressursse, nt väliseid võrguteenustajaid. 4. Võimalusel kasutab innovatiivseid lahendusi ning integreerib neid olemasolevatesse süsteemidesse ja teenustesse, arvestades turvameetmeid. 5. Annab kasutajale üle täielikult töökorras lahenduse (sh dokumentatsiooni), lähtudes tarkvara pakendamise ja levitamise nõuetest.	
B.3.6 Dokumentatsiooni koostamine (e-CF B5)	**EKR tase 5**
Tegevusnäitajad 1. Koostab tooteid, teenuseid, komponente või rakendusi kirjeldavaid dokumente (sh kasutusjuhendeid). 2. Toodete, rakenduste ja teenuste projekteerimisel, väljatöötamisel ja juurutamisel juhindub kõigist selleks vajalikest dokumentidest. 3. Dokumenteerimisel kasutab versioonihaldust, järgib tehnilise dokumenteerimise tavasid ja keelekasutust (sh EVS 8). 4. Dokumentide tutvustamisel sihtgrupile valib asjakohase stiili ja suhtluskanali (nt esitlus, netivideo, dokumendivormis kasutusjuhend). 5. Tagab kirjeldatava objekti funktsionaalsuste ja omaduste nõuetekohase dokumenteerimise. 6. Tagab oma vastutusala dokumentide ajakohasuse ja kehtivuse. 7. Vajadusel kehtestab oma vastutusalas dokumenteerimisnõuded.	
B.3.7 Kasutajatugi (e-CF C1)	**EKR tase 5**
Tegevusnäitajad	

1. Vastab kasutajate infoturbealastele küsimustele ja päringutele, registreerib asjakohase teabe. 2. Tuvastab turvaprobleemi olemuse küsitledes kasutajaid, analüüsides sümptomeid ning kasutades asjakohaseid IT tugirakendusi. 3. Otsib lahendusi kasutajatel esinenud turvaprobleemidele, kasutades selleks mitmesuguseid teabeallikaid. 4. Lahendab kasutajate turvaprobleemid kooskõlas veaparandusprotseduuridega. Vajadusel suunab probleemi lahendamiseks edasi. 5. Tõlgendab kasutaja turvaprobleeme süsteemselt, leiab neile lahendused. Kasutab vajalikke töövahendeid (kaugtoe tööriistu, seiresüsteeme) ning arvestab võimalikke kõrvaltoimeid. 6. Probleemi lahendamisel peab silmas lõpptulemust ja kliendi rahulolu.

B.3.8 Muudatuste tugi (e-CF C2)	**EKR tase 5**
Tegevusnäitajad 1. Analüüsib ja hindab talitluslike/tehniliste muudatuste mõju süsteemile. 2. Rakendab muudatusi konkreetsetes IT-lahendustes, lähtudes juhistest, heast tavast, oma kogemustest ning infoturbe alastest protseduuridest. 3. Koostab tarkvara- või riistvaramuudatuste käikuandmise ajakava, riske käsitledes arvestab infosüsteemi otstarvet ning käideldavusnõudeid. 4. Minimeerib muudatustest tingitud teenusekatkestusi, järgib määratletud teenusetasemelepet, lähtub äriprotsesside katkematu toimimise vajadusest. 5. Kasutab IT-lahenduste haldusvahendeid koostöös IT-lahenduste korrashoiu ja arendamise eest vastutavate meeskondadega. 6. Osaleb teabevahetuses infosüsteemide lahenduste korrashoiu ja arendamise eest vastutavate IT-meeskondadega.	

B.3.9 Teenuse andmine (e-CF C3)	**EKR tase 5**
Tegevusnäitajad 1. Oma pädevuse piires tagab IT-teenuse stabiilse, turvalise ning tõhusa toimimise vastavalt kokkulepitud teenusetasemele. 2. Hindab ennetus- ja turvameetmeid, rakendab neid; infoturbe- ja jõudlusnõuete täidetuse seireks kasutab seiresüsteeme. 3. Seirab süsteemide talitluslikke näitajaid, tuvastab turvaintsidendid ja teenuste tõrked. 4. Ajakohastab seire- ja haldustööriistu (nt skriptid, protseduurid), testib nende asjakohast tööd perioodiliselt. 5. Ajakohastab teenusega seotud dokumendid, registreerib kõik olulised sündmused ja intsidendid. 6. Teadaolevate infoturvariskide valguses analüüsib esmast teavet teenusetaset mõjutavatest sündmustest ning teavitab huvitatud osapooli. 7. Teeb ettepanekuid teenuse töökindluse parandamiseks ja turvataseme tõstmiseks. 8. Viib protsesse ellu kooskõlas organisatsiooni IKT teenuse strateegiaga.	

B.3.10 Intsidendi- ja probleemihaldus (e-CF C4)	**EKR tase 5**
Tegevusnäitajad: 1. Registreerib infoturbejuhtumid töövoohaldussüsteemi vahenditega, märgistab need etteantud tunnuste järgi ning intsidendi kriitilisuse põhjal. 2. Tuvastab soovimatud kõrvalekalded infosüsteemi normaalsest tööst. 3. Tagab tõendite rikkumatuse, võimaldades turvaintsidendi edasist uurimist (nt õiguskaitseorganite, CERT, sisekontrolli poolt). 4. Vajadusel teavitab töötajaid ja partnereid juba toimunud või võimaliku intsidendi mõjust ning teeb juhtkonnale kerksusettepanekuid. 5. Tuvastab turvaintsidendi algpõhjused ja lahendab intsidendi lähtudes organisatsiooni protseduuridest. 6. Intsidendi mõju hindamisel arvestab infosüsteemi elementide ja süsteemi taristu omavahelisi seoseid ning toimet äriprotsessidele. 7. Suunab korduva intsidendi probleemihaldusse. 8. Osaleb IT ja infoturbehaldussüsteemi auditites ning on kaasatud riskihaldustoimingutesse.	

B.3.11 Infoturbestrateegia väljatöötamises osalemine (e-CF D1)	**EKR tase 5**
Tegevusnäitajad 1. Osaleb infoturbestrateegia väljatöötamises, lähtudes enamlevinud standarditest ja infoturbe heast tavast. 2. Osaleb olemasoleva olukorra kaardistamises ja annab soovitusi asjakohaste turvanõuete täitmiseks.	

B.3.12 Personaliarendus (e-CF D9)	EKR tase 5
Tegevusnäitajad 1. Annab sisendi infoturbealase koolitusvajaduse kaardistamisse. 2. Annab soovitused koolituste läbiviimiseks sobivate teenustajate osas. 3. Juhendab üksikisikuid ja meeskondi turvanõuete võimalike rikkumiste ennetamiseks ning nõustab neid intsidentide järgselt.	
B.3.13 Riskihaldus (e-CF E3)	**EKR tase 5**
Tegevusnäitajad 1. Kaardistab keskkonnapõhised infoturvariskid (veeb, võrk, pilv, mobiilsed seadmed jne). 2. Annab sisendi riskiregistri koostamisse ja riskiohjeplaanide haldusse, lähtudes heast tavast ja levinud raamistikest. 3. Viib ellu riskide leevendamiseks ja vältimiseks vajalikke tegevusi, arvestades koostatud plaane.	
B.3.14 Infoturbe haldamine (e-CF E8)	**EKR tase 5**
Tegevusnäitajad 1. Osaleb infoturbehalduses vastavalt oma pädevusele, sh intsidendihaldus, osalemine auditites. 2. Osaleb infovarade ja nende nõrkuste kaardistamisel, väiksemas organisatsioonis koordineerib neid tegevusi. 3. Annab sisendit infovaradele turvaklasside määramisel ning infovarade nõuetekohaseks käsitlemiseks. 4. Osaleb infoturvameetmete rakendusplaani koostamisel, lähtudes infoturbepoliitikast. 5. Määratleb andmete, varukoopiate, teenuseühenduste krüpteerimisvajaduse, lähtudes ärilistest vajadustest ja organisatsioonile kehtestatud nõuetest. 6. Koostöös IT-meeskonnaga koostab, haldab ja testib IT-süsteemide varundus- ja taasteplaane, lähtudes heast tavast ja tunnustatud raamistikest.	

C-osa
ÜLDTEAVE JA LISAD

C.1 Teave kutsestandardi koostamise ja kinnitamise kohta ning viide ametite klassifikaatorile	
1. Kutsestandardi tähis kutseregistris	08-02112023-2.7/2k
2. Kutsestandardi koostajad	Anto Veldre, Cybernetica AS Rain Ottis, Tallinna Tehnikaülikool Triin Muulmann, Kehtna Kutsehariduskeskus Holger Rünkaru, Telia Eesti AS Kristjan Leotoots, Pärnu Kutsehariduskeskus Allan Ild, Followercase OÜ
3. Kutsestandardi kinnitaja	Infotehnoloogia ja Telekommunikatsiooni Kutsenõukogu
4. Kutsenõukogu otsuse number	25
5. Kutsenõukogu otsuse kuupäev	02.11.2023
6. Kutsestandard kehtib kuni	01.11.2028
7. Kutsestandardi versiooni number	2
8. Viide Ametite Klassifikaatorile (ISCO 08)	2529 Andmebaasi ja arvutivõrgu tippspetsialistid, mujal liigitamata
9. Viide Euroopa kvalifikatsiooniraamistikule (EQF)	5
C.2 Kutsenimetus võõrkeeles	
Inglise keeles	ICT Security Specialist, EstQF Level 5
C.3 Lisad	
Lisa 1 Keelte oskustasemete kirjeldused	
Lisa 2 Digipädevuste enesehindamisskaala	